02.02.01

JP 01/772

#4

EU

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ７月１１日

出 願 番 号
Application Number: 特願２０００－２０９６７５

出 願 人
Applicant (s): ソニー株式会社

09/937797

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００１年 ３月 ２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２００１－３０１５１６２

【書類名】　特許願
【整理番号】　0000065405
【提出日】　平成12年 7月11日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/60
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　金巻　裕史
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　中村　嘉秀
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　佐竹　清
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　出井　伸之
【代理人】
　【識別番号】　100094053
　【弁理士】
　【氏名又は名称】　佐藤　隆久
【手数料の表示】
　【予納台帳番号】　014890
　【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707389

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証装置、処理装置、認証システムおよびその方法

【特許請求の範囲】

【請求項１】

認証要求に応じて認証処理を行う認証装置であって、

利用者を識別するための第１の識別情報と、前記認証要求の送信元の装置を識別する第２の識別情報とを含む前記認証要求を受信する受信手段と、

前記第１の識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記認証要求に応じて認証処理を行う認証処理手段と、

前記認証要求に含まれる前記第１の識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記第２の識別情報とを対応付けて送信する送信手段と

を有する認証装置。

【請求項２】

前記受信手段は、暗号化された前記第１の識別情報および前記第２の識別情報を含む前記認証要求を受信し、

前記認証装置は、

前記受信した認証要求に含まれる前記第１の識別情報および前記第２の識別情報を復号する復号手段

をさらに有する請求項１に記載の認証装置。

【請求項３】

前記受信手段は、前記利用者に関する課金処理に用いられる第３の識別情報をさらに含む前記認証要求を受信する

請求項１に記載の認証装置。

【請求項４】

前記第１の識別情報は、登録した利用者に予め割り当てられた識別子である

請求項１に記載の認証装置。

【請求項５】

前記第２の識別情報は、前記装置の製造元で付された当該装置を一意に識別可能な識別子である

請求項１に記載の認証装置。

【請求項６】

ネットワークを介して行われる取り引きに関する認証処理を行う認証装置であって、

利用者を識別するための第１の識別情報と、取り引きの内容を示す取り引き情報と、前記認証要求の送信元の装置を識別する第２の識別情報とを含み前記取り引きを行う利用者による前記認証要求を受信する受信手段と、

前記第１の識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記受信した認証要求に含まれる前記取り引き情報を前記認証要求によって指定された利用者の装置に送信し、当該指定された利用者の装置からの応答に応じて、所定の認証処理を行う認証処理手段と、

前記認証要求に含まれる前記第１の識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記第２の識別情報とを対応付けて送信する送信手段と

を有する認証装置。

【請求項７】

前記認証処理手段は、

前記取り引き情報に当該認証装置の認証結果を示す署名情報を付して前記指定された利用者の装置に送信し、前記指定された利用者からの応答に応じて、当該認証装置の署名情報を前記認証処理の結果として生成する

請求項６に記載の認証装置。

【請求項８】

前記記憶手段は、

前記認証要求を発した利用者と前記指定された利用者との間の取り引きの履歴

情報を記憶する

請求項６に記載の認証装置。

【請求項９】

前記受信手段は、暗号化された前記第１の識別情報および前記第２の識別情報を含む前記認証要求を受信し、

前記認証装置は、

前記受信した認証要求に含まれる前記第１の識別情報および前記第２の識別情報を復号する復号手段

をさらに有する請求項６に記載の認証装置。

【請求項１０】

前記受信手段は、前記利用者に関する課金処理に用いられる第３の識別情報をさらに含む前記認証要求を受信する

請求項６に記載の認証装置。

【請求項１１】

前記取り引きに関する認証に対しての課金処理を行う課金処理手段

をさらに有する請求項６に記載の認証装置。

【請求項１２】

ネットワークを介して行われる取り引きに関する認証要求を行う処理装置であって、

利用者を識別するための第１の識別情報と、当該処理装置を識別するための第２の識別情報とを含む前記認証要求を送信する送信手段と、

認証要求の送信元の装置を識別するための識別情報を含む認証応答を受信する受信手段と、

前記第２の識別情報と、前記認証応答に含まれる識別情報とが一致するか否かを判断する制御手段と

を有する処理装置。

【請求項１３】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する

請求項１２に記載の処理装置。

【請求項１４】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置に所定の通知を行う

請求項１２に記載の処理装置。

【請求項１５】

ネットワークを介して接続される処理装置および認証装置を有する認証システムであって、

前記認証装置は、

利用者を識別するための第１の識別情報と、前記認証要求の送信元の装置を識別する第２の識別情報とを含む前記認証要求を受信する受信手段と、

前記第１の識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記認証要求に応じて認証処理を行う認証処理手段と、

前記認証要求に含まれる前記第１の識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記第２の識別情報とを含む認証応答を送信する送信手段と

を有し、

前記処理装置は、

前記第１の識別情報と、当該処理装置を識別するための前記第２の識別情報とを含む前記認証要求を送信する送信手段と、

前記認証応答を受信する受信手段と、

当該処理装置の前記第２の識別情報と、前記認証応答に含まれる前記第２の識別情報とが一致するか否かを判断する制御手段と

を有する

認証システム。

【請求項１６】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する

請求項１５に記載の認証システム。

【請求項１７】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置に所定の通知を行う

請求項１５に記載の認証システム。

【請求項１８】

ネットワークを介して接続される処理装置および認証装置を有する認証方法であって、

利用者を識別するための第１の識別情報と、当該処理装置を識別するための第２の識別情報とを含む認証要求を前記処理装置から前記認証装置に送信し、

前記認証装置において前記認証要求に応じて認証処理を行い、

前記認証装置から、前記認証要求に含まれる前記第１の識別情報に対応する前記送信先の情報によって特定された前記処理装置に、前記認証処理の結果と前記認証要求に含まれる前記第２の識別情報とを含む認証応答を送信し、

前記処理装置において、前記認証装置から受信した前記認証応答に含まれる前記第２の識別情報と、当該処理装置の前記第２の識別情報と、前記認証応答に含まれる前記第２の識別情報とが一致するか否かを判断する

認証方法。

【請求項１９】

前記処理装置は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証装置に通知する

請求項１８に記載の認証方法。

【請求項２０】

前記処理装置は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置に所定の通知を行う

請求項１８に記載の認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子商取引情報を認証する認証装置、処理装置、認証システムおよびその方法に関する。

【０００２】

【従来の技術】

インターネットなどのネットワークを介して商品等の販売や代金の決済を行う電子商取引が普及している。

このような電子商取引を用いて利用者が商品等を購入する場合には、例えば、利用者が店舗や各家庭に設置されたパーソナルコンピュータなどの発注者端末装置を操作して、ネットワークを介して、商品等の販売を行うサーバ装置にアクセスを行う。これにより、サーバ装置から発注者端末装置に商品の写真、特性および価格などの情報が提供され、発注者端末装置のディスプレイに表示される。利用者は、このような情報を見ながら、購入を希望する商品等を選択し、選択した商品等の発注処理を行う。発注処理は、利用者個人を特定する個人ＩＤ情報、発注する商品等を指定した情報およびその決済方法等の情報を、発注者端末装置を操作して入力し、これをネットワークを介してサーバ装置に送信する。

【０００３】

このような電子商取引では、ネットワーク銀行などが、ネットワークを介した取り引きに関しての決済業務を行うが、当該決済を行うに当たって、決済対象となる電子商取引の内容の正当性が認証されている必要がある。

従って、電子商取引では、このような電子商取引の内容の正当性を認証する処理を行う認証装置が用いられる。当該認証装置を用いた認証業務は、ネットワーク銀行、あるいは他の信頼性のある機関が行う。

【０００４】

【発明が解決しようとする課題】

ところで、上述したような認証装置では、例えば、個人ＩＤ情報を他人が不正

に取得した場合に、当該他人は、その個人ＩＤ情報を用いて、認証装置に対して認証要求を出すことができ、不正な取り引きが行われてしまう可能性があるという問題がある。

【０００５】

本発明は上述した従来技術の問題点に鑑みてなされ、不正に取得した他人の個人ＩＤ情報に基づいて不正な認証手続が行われることを回避する認証装置、処理装置、認証システムおよびその方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第１の発明の認証装置は、認証要求に応じて認証処理を行う認証装置であって、利用者を識別するための第１の識別情報と、前記認証要求の送信元の装置を識別する第２の識別情報とを含む前記認証要求を受信する受信手段と、前記第１の識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記認証要求に応じて認証処理を行う認証処理手段と、前記認証要求に含まれる前記第１の識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記第２の識別情報とを対応付けて送信する送信手段とを有する。

【０００７】

第１の発明の認証装置の作用は以下のようになる。

例えば、利用者が端末装置などを操作して当該端末装置から送信された、利用者を識別するための第１の識別情報と、認証要求の送信元の装置を識別する第２の識別情報とを含む前記認証要求が受信手段で受信される。

次に、当該受信された前記認証要求に応じた認証処理が認証処理手段で行われる。

次に、送信手段によって、前記認証要求に含まれる前記第１の識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含ま

れる前記第２の識別情報とが対応付けて送信手段から送信される。

【０００８】

また、第１の発明の認識装置は、好ましくは、前記受信手段は、暗号化された前記第１の識別情報および前記第２の識別情報を含む前記認証要求を受信し、前記認証装置は、前記受信した認証要求に含まれる前記第１の識別情報および前記第２の識別情報を復号する復号手段をさらに有する。

【０００９】

また、第１の発明の認証装置は、好ましくは、前記受信手段は、前記利用者に関する課金処理に用いられる第３の識別情報をさらに含む前記認証要求を受信する。

【００１０】

また、第１の発明の認証装置は、好ましくは、前記第１の識別情報は、登録した利用者に予め割り当てられた識別子である。

【００１１】

また、第１の発明の認証装置は、好ましくは、前記第２の識別情報は、前記装置の製造元で付された当該装置を一意に識別可能な識別子である。

【００１２】

第２の発明の認証装置は、ネットワークを介して行われる取り引きに関する認証処理を行う認証装置であって、利用者を識別するための第１の識別情報と、取り引きの内容を示す取り引き情報と、前記認証要求の送信元の装置を識別する第２の識別情報とを含み前記取り引きを行う利用者による前記認証要求を受信する受信手段と、前記第１の識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記受信した認証要求に含まれる前記取り引き情報を前記認証要求によって指定された利用者の装置に送信し、当該指定された利用者の装置からの応答に応じて、所定の認証処理を行う認証処理手段と、前記認証要求に含まれる前記第１の識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記第２の識別情報とを対応付けて送信する送信手段とを有する。

【００１３】

第２の発明の認証装置の作用は以下のようになる。

利用者を識別するための第１の識別情報と、取り引きの内容を示す取り引き情報と、前記認証要求の送信元の装置を識別する第２の識別情報とを含み前記取り引きを行う利用者による前記認証要求が受信手段で受信される。

次に、認証処理手段によって、前記受信した認証要求に含まれる前記取り引き情報が前記認証要求によって指定された利用者の装置に送信され、当該指定された利用者の装置からの応答に応じて、所定の認証処理が行われる。

次に、送信手段によって、前記認証要求に含まれる前記第１の識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記第２の識別情報とを対応付けて送信手段から送信される。

【００１４】

また、第２の発明の認証装置は、好ましくは、前記認証処理手段は、前記取り引き情報に当該認証装置の認証結果を示す署名情報を付して前記指定された利用者の装置に送信し、前記指定された利用者からの応答に応じて、当該認証装置の署名情報を前記認証処理の結果として生成する。

【００１５】

また、第２の発明の認証装置は、好ましくは、前記記憶手段は、前記認証要求を発した利用者と前記指定された利用者との間の取り引きの履歴情報を記憶する。

【００１６】

また、第２の発明の認証装置は、好ましくは、前記受信手段は、暗号化された前記第１の識別情報および前記第２の識別情報を含む前記認証要求を受信し、前記認証装置は、前記受信した認証要求に含まれる前記第１の識別情報および前記第２の識別情報を復号する復号手段をさらに有する。

【００１７】

また、第２の発明の認証装置は、好ましくは、前記受信手段は、前記利用者に関する課金処理に用いられる第３の識別情報をさらに含む前記認証要求を受信す

る。

【００１８】

また、第２の発明の認証装置は、好ましくは、前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する。

【００１９】

また、第３の発明の処理装置は、ネットワークを介して行われる取り引きに関する認証要求を行う処理装置であって、利用者を識別するための第１の識別情報と、当該処理装置を識別するための第２の識別情報とを含む前記認証要求を送信する送信手段と、認証要求の送信元の装置を識別するための識別情報を含む認証応答を受信する受信手段と、前記第２の識別情報と、前記認証応答に含まれる識別情報とが一致するか否かを判断する制御手段とを有する。

【００２０】

また、第３の発明の処理装置は、好ましくは、前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する。

【００２１】

また、第３の発明の処理装置は、好ましくは、前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引きの取り引き先の装置に所定の通知を行う。

【００２２】

また、第４の発明の認証システムは、ネットワークを介して接続される処理装置および認証装置を有する認証システムであって、前記認証装置は、利用者を識別するための第１の識別情報と、前記認証要求の送信元の装置を識別する第２の識別情報とを含む前記認証要求を受信する受信手段と、前記第１の識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記認証要求に応じて認証処理を行う認証処理手段と、前記認証要求に含まれる前記第１の識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記第２の識別情報とを含む認証応答を送信する送信手段と

を有し、前記処理装置は、前記第１の識別情報と、当該処理装置を識別するための前記第２の識別情報とを含む前記認証要求を送信する送信手段と、前記認証応答を受信する受信手段と、当該処理装置の前記第２の識別情報と、前記認証応答に含まれる前記第２の識別情報とが一致するか否かを判断する制御手段とを有する。

【００２３】

また、第５の発明の認証方法は、ネットワークを介して接続される処理装置および認証装置を有する認証方法であって、利用者を識別するための第１の識別情報と、当該処理装置を識別するための第２の識別情報とを含む認証要求を前記処理装置から前記認証装置に送信し、前記認証装置において前記認証要求に応じて認証処理を行い、前記認証装置から、前記認証要求に含まれる前記第１の識別情報に対応する前記送信先の情報によって特定された前記処理装置に、前記認証処理の結果と前記認証要求に含まれる前記第２の識別情報とを含む認証応答を送信し、前記処理装置において、前記認証装置から受信した前記認証応答に含まれる前記第２の識別情報と、当該処理装置の前記第２の識別情報と、前記認証応答に含まれる前記第２の識別情報とが一致するか否かを判断する。

【００２４】

また、第５の発明の認証方法は、好ましくは、前記処理装置は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証装置に通知する。

【００２５】

【発明の実施の形態】

以下、本発明の実施形態に係わるトランザクション認証システムについて説明する。

図１は、本実施形態のトランザクション認証システム１０１の全体構成図である。

図１に示すように、トランザクション認証システム１０１では、例えば、発注者３１の発注者端末装置１１と、受注者３３の受注者端末装置１５と、ネットワーク銀行４０の認証装置５０とが、インターネットなどのネットワーク（通信網

）を介して接続されており、発注者３１と受注者３３との間のトランザクション（取り引き）の正当性を認証装置５０で認証する。

なお、当該ネットワークに接続されている発注者端末装置１１および発注者受注者端末装置１５の数は任意である。

【００２６】

本実施形態では、発注者端末装置１１が第３の発明の処理装置に対応し、認証装置５０が本発明の認証装置に対応している。

【００２７】

本実施形態では、例えば、発注者３１および受注者３３とネットワーク銀行４０との間で認証を行うことに関しての契約が成されている。また、発注者３１と引き落とし銀行４２との間では、例えば、ネットワーク銀行４０によって認証された取り引きに関しての引き落としを行う旨の契約がなされている。また、ネットワーク銀行４０と保険会社４３との間では、ネットワーク銀行４０が係わった電子商取引によって生じた損害についての保険契約がなされている。

【００２８】

以下、トランザクション認証システム１０１を構成する各装置について説明する。

〔発注者端末装置１１〕

図２に示すように、発注者端末装置１１は、例えば、発注者３１の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部６１、送信部６２、暗号化部６３、復号部６４、記憶部６５、制御部６６および署名検証部６７を有する。

なお、発注者端末装置１１は、例えば、発注者３１が使用する際に、発注者３１の指紋等の身体的特徴から得られる情報と、予め記憶部６５に予め記憶してある身体的特徴を示す情報とを比較することで、発注者３１が正当な利用者であることを認証する生体認証部を有していてもよい。

【００２９】

ここで、受信部６１が第３の発明の受信手段に対応し、送信部６２が第３の発明の送信手段に対応し、制御部６６が第３の発明の制御手段に対応している。

【００３０】

受信部６１は、ネットワークを介して認証装置５０から情報あるいは要求を受信する。

送信部６２は、ネットワークを介して認証装置５０に情報あるいは要求を送信する。

また、受信部６１および送信部６２は、受注者３３が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部６３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部６４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部６５は、製造元で受注者端末装置１５に付された装置ＩＤ情報$ＩＤ_{M}$（本発明の第２の識別情報）と、発注者３１が作成した秘密鍵$K_{33,S}$などを格納する。

署名検証部６７は、例えば、認証装置５０が作成した署名情報を、ネットワーク銀行４０の公開鍵$K_{40,P}$を用いて検証する。

制御部６６は、発注者端末装置１１内の各構成要素の処理を統括的に制御する。

【００３１】

制御部６６は、例えば、発注者３１による操作に応じて、発注情報ａ１と、個人キー情報ｋ１（本発明の第１の識別情報）と、個人ＩＤ情報ＩＤ１（本発明の第１の識別情報）と、記憶部６５から読み出した装置ＩＤ情報$ＩＤ_{M}$との全体に対してを暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求Ｉｎｆ１を生成する。

また、制御部６６は、例えば、認証要求Ｉｎｆ１を認証装置５０に送信した後に、認証装置５０から認証応答Ｉｎｆ４を受信したときに、認証応答Ｉｎｆ４に含まれる認証要求の送信元の装置を示す装置ＩＤ情報$ＩＤ_{M}$と、記憶部６５から読み出した発注者端末装置１１の装置ＩＤ情報$ＩＤ_{M}$とが一致するか否かを検出し、一致している場合には、正当な取り引きが行われていると判断し、不一致の場合には、不正な取り引きが行われたと判断して、その旨を受注者端末装置１５

および認証装置５０の少なくとも一方に通知する。

【００３２】

〔受注者端末装置１５〕

図３に示すように、受注者端末装置１５は、サイバーモール(Cyber Moll)などに店舗を出している受注者３３が使用するサーバ装置であり、受信部７１、送信部７２、暗号化部７３、復号部７４、記憶部７５、制御部７６および署名検証部７７を有する。

受信部７１は、ネットワークを介して認証装置５０から情報あるいは要求を受信する。

送信部７２は、ネットワークを介して認証装置５０に情報あるいは要求を送信する。

また、受信部７１および送信部７２は、発注者端末装置１１からのアクセスに応じて、例えば、記憶部７５から読み出した受注者３３が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置１１に送信する。

暗号化部７３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部７４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部７５は、受注者３３が作成した秘密鍵$K_{33,S}$などを格納する。

制御部７６は、受注者端末装置１５内の各構成要素の処理を統括的に制御する。

署名検証部７７は、例えば、ネットワーク銀行４０の公開鍵$K_{40,P}$を用いて、認証装置５０が作成した署名情報の検証を行う。

【００３３】

〔認証装置５０〕

図４に示すように、認証装置５０は、受信部８１、送信部８２、暗号化部８３、復号部８４、記憶部８５、制御部８６、署名作成部８７および課金処理部８８を有する。

【００３４】

ここで、受信部８１が第１および第２の発明の受信手段に対応し、送信部８２が第１および第２の発明の送信手段に対応し、記憶部８５が第１および第２の発

明の記憶手段に対応し、制御部８６が第１および第２の発明の認証処理手段に対応している。

【００３５】

受信部８１は、ネットワークを介して発注者端末装置１１および受注者端末装置１５から情報あるいは要求を受信する。

送信部８２は、ネットワークを介して発注者端末装置１１および受注者端末装置１５に情報あるいは要求を送信する。

暗号化部８３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部８４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部８５は、発注者３１がネットワーク銀行４０と契約したときに、発注者３１の個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、発注者端末装置１１のアドレス（または、発注者端末装置１１が配設された家庭のセット・トップ・ボックスのアドレスあるいは電話番号等）との対応表を記憶する。また、記憶部８５は、例えば、発注者３１および受注者３３がネットワーク銀行４０と契約をしたときに、発注者３１が作成した秘密鍵$K_{31,S}$に対応する公開鍵$K_{31,P}$、並びに受注者３３が作成した秘密鍵$K_{33,S}$に対応する公開鍵$K_{33,P}$などを格納する。

制御部８６は、認証装置５０内の各構成要素の処理を統括的に制御する。

署名作成部８７は、ネットワーク銀行４０の秘密鍵$K_{40,S}$を用いて署名情報の作成を行う。

課金処理部８８は、発注者３１による取り引きに関する認証に対しての課金処理を行う。

認証装置５０の各構成要素の詳細な処理については、後述する動作例で記載する。

【００３６】

以下、トランザクション認証システム１０１の動作例を説明する。

当該動作例を開始する前提として、発注者３１とネットワーク銀行４０との間で所定の契約が結ばれ、ネットワーク銀行４０は、発注者３１に対して、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１を発行する。

ネットワーク銀行４０は、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、発注

者端末装置１１のアドレス（または、発注者端末装置１１が配設された家庭のセット・トップ・ボックスのアドレスあるいは電話番号等）との対応表を図４に示す認証装置５０の記憶部８５に記憶する。ここで、個人キー情報ｋ１は、例えば、ネットワーク銀行４０と契約した契約者（発注者３１）の契約番号などの個人情報を示す識別子である。また、個人ＩＤ情報ＩＤ１は、発注者３１の銀行口座番号などの課金に係わる情報を示す識別子である。

【００３７】

また、ネットワーク銀行４０は、自らの秘密鍵$K_{40,S}$を図４に示す認証装置５０の記憶部８５に記憶すると共に、当該秘密鍵$K_{40,S}$に対応する公開鍵$K_{40,P}$を発注者端末装置１１および受注者端末装置１５に送信する。発注者端末装置１１は、公開鍵$K_{40,P}$を図２に示す記憶部６５に記憶する。受注者端末装置１５は、公開鍵$K_{40,P}$を図３に示す記憶部７５に記憶する。

【００３８】

また、受注者３３とネットワーク銀行４０との間で所定の契約が結ばれ、ネットワーク銀行４０は、受注者３３に対して、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２を発行する。ネットワーク銀行４０は、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２の対応表を図４に示す認証装置５０の記憶部８５に記憶する。

【００３９】

図５は、トランザクション認証システム１０１の動作例を説明するための図である。

ステップＳＴ１１：

図１に示す発注者３１は、例えばネットワーク上の商店である受注者３３に商品を発注する場合に、発注する商品名および数量などを示す発注情報ａ１と、発注者３１の個人キー情報ｋ１と、発注者３１の個人ＩＤ情報ＩＤ１とを、図示しない操作手段を操作して発注者端末装置１１に入力する。なお、発注情報ａ１には、受注者３３を特定する情報が含まれている。

次に、図２に示す発注者端末装置１１の暗号化部６３は、記憶部６５から読み出したネットワーク銀行４０の公開鍵$K_{40,P}$を用いて、発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、記憶部６５から読み出した装置ＩＤ情報

ID_Mとの全体に対してを暗号化を行い、当該暗号化した情報を格納した認証要求Ｉｎｆ１（本発明の第１の要求）を、送信部６２からネットワークを介して、図１に示すネットワーク銀行４０の認証装置５０に送信する。

【００４０】

ステップＳＴ１２：

図４に示す認証装置５０は、発注者端末装置１１からの認証要求Ｉｎｆ１を受信部８１が受信すると、記憶部８５からネットワーク銀行４０の秘密鍵$K_{40,S}$を読み出し、復号部８４において、当該秘密鍵$K_{40,S}$を用いて認証要求Ｉｎｆ１を復号する。

次に、認証装置５０は、制御部８６の制御に基づいて、上記復号した認証要求Ｉｎｆ１に格納された発注情報ａ１および個人キー情報ｋ１を格納した情報Ｉｎｆ１’とについて、記憶部８５から読み出した自らの秘密鍵$K_{40,S}$を用いて署名情報Ａｕ１を作成する。

次に、認証装置５０は、情報Ｉｎｆ１’および署名情報Ａｕ１を格納した要求Ｉｎｆ２を生成する。

次に、暗号化部８３は、図４に示す記憶部８５から読み出した受注者３３の公開鍵$K_{33,P}$を用いて、上記生成した要求Ｉｎｆ２を暗号化した後に、送信部８２から、ネットワークを介して受注者端末装置１５に送信する。

【００４１】

ステップＳＴ１３：

受注者端末装置１５の復号部７４は、認証装置５０からの要求Ｉｎｆ２を受信部７１が受信すると、記憶部７５から読み出した自らの秘密鍵$K_{33,S}$を用いて、要求Ｉｎｆ２を復号する。

次に、受注者端末装置１５の署名検証部７７は、上記復号した要求Ｉｎｆ２に格納された署名情報Ａｕ１を、記憶部７５から読み出した認証装置５０の公開鍵$K_{40,P}$を用いて検証する。

【００４２】

受注者端末装置１５の制御部７６は、署名検証部が上記検証の結果、署名情報Ａｕ１の正当性が認証されると、要求Ｉｎｆ２に格納された情報Ｉｎｆ１’を図

３に示す記憶部７５に記憶する。受注者３３は、情報Ｉｎｆ１’内の発注情報ａ１に基づいて、発注者３１への商品等の発送予定などを示す受注確認情報ｃ１を生成する。

次に、制御部７６は、要求Ｉｎｆ２、受注確認情報ｃ１および自らの個人キー情報Ｚを格納した応答Ｉｎｆ３を生成する。

次に、受注者端末装置１５の送信部７２は、上記生成した応答Ｉｎｆ３を、記憶部７５から読み出したネットワーク銀行４０の公開鍵$K_{40,P}$を用いて暗号化部７３で暗号化した後に、送信部７２から、ネットワークを介して認証装置５０に送信する。

受注者３３は、例えば、要求Ｉｎｆ２に格納された情報Ｉｎｆ１’内の発注情報ａ１に基づいて、発注者３１が発注した商品等を発注者３１に発送したり、発注者３１が注文したサービスを発注者３１に提供する。

【００４３】

ステップＳＴ１４：

認証装置５０の復号部８４は、受注者端末装置１５からの応答Ｉｎｆ３を受信部８１が受信すると、記憶部８５から読み出した自らの秘密鍵$K_{40,S}$を用いて、Ｉｎｆ３を復号し、要求Ｉｎｆ１に格納された発注情報ａ１と、当該復号されたＩｎｆ３に格納された受注者３３の個人キー情報Ｚとを用いて、所定の取り引き履歴情報を作成し、これを記憶部８５に格納する。当該履歴情報は、ネットワーク銀行４０が、発注者３１に対して決済を行う際に用いられる。

また、認証装置５０の署名作成部８７は、ステップＳＴ１３で受信した応答Ｉｎｆ３について、自らの秘密鍵$K_{40,S}$を用いて署名情報Ａｕ２を作成する。

次に、認証装置５０の制御部８６は、応答Ｉｎｆ３および署名情報Ａｕ２を格納した認証応答Ｉｎｆ４を作成する。

次に、認証装置５０の暗号化部８３は、上記作成し認証た応答Ｉｎｆ４を、記憶部８５から読み出した発注者３１の公開鍵$K_{31,P}$を用いて暗号化した後に、送信部８２から、ネットワークを介して発注者端末装置１１に送信する。

【００４４】

ステップＳＴ１５：

発注者端末装置１１では、受信した認証応答Ｉｎｆ４を、図２示す記憶部６５から読み出した発注者３１の秘密鍵$K_{31,S}$を用いて復号部６４で復号する。

次に、発注者端末装置１１の署名検証部６６は、当該復号した認証応答Ｉｎｆ４に格納された署名情報Ａｕ２を、記憶部６５から読み出したネットワーク銀行４０の公開鍵$K_{40,P}$を用いて検証すると共に、Ｉｎｆ４内の発注情報ａ１内に記述された装置ＩＤ情報$ＩＤ_M$が図２に示す発注者端末装置１１の記憶部６５に記憶されている自らの装置ＩＤ情報$ＩＤ_M$と一致するかを判断し、一致すると判断した場合には、受注者３３との間の当該取り引きが正当に行われたことを確認する。　発注者端末装置１１は、Ｉｎｆ４内の発注情報ａ１内に記述された装置ＩＤ情報$ＩＤ_M$が図２に示す発注者端末装置１１の記憶部６５に記憶されている自らの装置ＩＤ情報$ＩＤ_M$と一致しないと判断した場合には、例えば、認証応答Ｉｎｆ４を格納した不正発注通知Ｉｎｆ５を認証装置５０および受注者端末装置１５の少なくとも一方に送信する。

これにより、認証装置５０および受注者端末装置１５は、発注者端末装置１１が発した認証要求Ｉｎｆ１に対応した発注を取り消す。

また、発注者端末装置１１は、不正発生通知Ｉｎｆ５を、図１に示す引き落とし銀行４２に送信してもよい。

【００４５】

以上説明したように、トランザクション認証システム１０１によれば、認証要求Ｉｎｆ１内に、個人ＩＤ情報ＩＤ１の他に当該認証要求を出した装置ＩＤ情報$ＩＤ_M$を自動的に挿入し、認証装置５０において、認証要求Ｉｎｆ１に含まれる発注者３１が使用する発注者端末装置１１のアドレスに、認証結果を含む認証応答Ｉｎｆ４を送信し、当該認証応答Ｉｎｆ４内に当該認証要求を出した装置ＩＤ情報$ＩＤ_M$を格納することで、発注者端末装置１１では、認証応答Ｉｎｆ４に格納された当該認証要求を出した装置ＩＤ情報$ＩＤ_M$と自らの装置ＩＤ情報$ＩＤ_M$とが一致するか否かを判断することで、自らの個人ＩＤ情報ＩＤ１を用いた不正な認証要求（なりすまし）が発生したことを検出できる。

その結果、トランザクション認証システム１０１によれば、他人の個人ＩＤ情報を用いた不正な取り引きを効果的に抑制できる。

【００４６】

上述したように、トランザクション認証システム１０１によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などを費用を低額にでき、電子商取引をさらに普及させることが可能になる。

【００４７】

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、発注者端末装置１１において、認証応答Ｉｎｆ４内の発注情報ａ１内に記述された装置ＩＤ情報$ＩＤ_{M}$が図２に示す発注者端末装置１１の記憶部６５に記憶されている自らの装置ＩＤ情報$ＩＤ_{M}$と一致するかを判断し、一致しないと判断した場合には、例えば、認証応答Ｉｎｆ４を格納した不正発注通知Ｉｎｆ５を認証装置５０および受注者端末装置１５の少なくとも一方に送信する場合を例示したが、例えば、一致しない旨（不正な取り引きが行われた旨）を発注者端末装置１１のディスプレイなどに表示し、発注者３１にその旨を知らせるようにしてもよい。

また、発注者端末装置１１において、上述した装置ＩＤ情報$ＩＤ_{M}$の一致を判断するのではなく、発注者３１が判断してもよい。

また、発注者端末装置１１が配設された家庭にホーム・ゲートウェイ(Home Gateway)が設置されている場合には、ホーム・ゲートウェイに発注者端末装置１１の装置ＩＤ情報$ＩＤ_{M}$を登録しておき、認証装置５０からの認証応答Ｉｎｆ４をホーム・ゲートウェイが受信したときに、ホーム・ゲート・ウェイにおいて、上記装置ＩＤ情報$ＩＤ_{M}$の一致の判断を行ってもよい。

【００４８】

また、上述した実施形態では、ネットワーク銀行４０が、認証装置５０を用いて、トランザクション（取り引き）の認証業務を行う場合を例示したが、ネットワーク銀行４０とは別の機関が、認証装置５０を用いてトランザクションの認証業務を行うようにしてもよい。

【００４９】

また、上述した実施形態では、図５に示すステップＳＴ１１のように、暗号化

された発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、装置ＩＤ情報$ＩＤ_M$とを含む認証要求Ｉｎｆ１を、発注者端末装置１１から認証装置５０に送信する場合を例示したが、発注情報ａ１と、個人キー情報ｋ１と、装置ＩＤ情報$ＩＤ_M$とを含む認証要求Ｉｎｆ１を、発注者端末装置１１から認証装置５０に送信してもよい。このようにすれば、課金に係わる情報である個人ＩＤ情報ＩＤ１はネットワークを介して伝送されないため、ネットワーク上で個人ＩＤ情報ＩＤ１が不正に取得され、悪用されることを回避できる。

【００５０】

また、上述した実施形態では、図２に示す発注者端末装置１１の暗号化部６３において、記憶部６５から読み出した所定の暗号鍵を用いて、発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、記憶部６５から読み出した装置ＩＤ情報$ＩＤ_M$との全体に対してを暗号化を行う場合を例示したが、発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、記憶部６５から読み出した装置ＩＤ情報$ＩＤ_M$とのそれぞれについて個別に暗号化を行ってもよい。

【００５１】

【発明の効果】

以上説明したように、本発明によれば、不正に取得した他人の識別情報（個人ＩＤ情報）に基づいて不正な認証手続が行われることを回避する認証装置、処理装置、認証システムおよびその方法を提供できる。

【図面の簡単な説明】

【図１】

図１は、本発明の実施形態のトランザクション認証システムの全体構成図である。

【図２】

図２は、図１に示す発注者端末装置の構成図である。

【図３】

図３は、図１に示す受注者端末装置の構成図である。

【図４】

図４は、図１に示す認証装置の構成図である。

【図５】

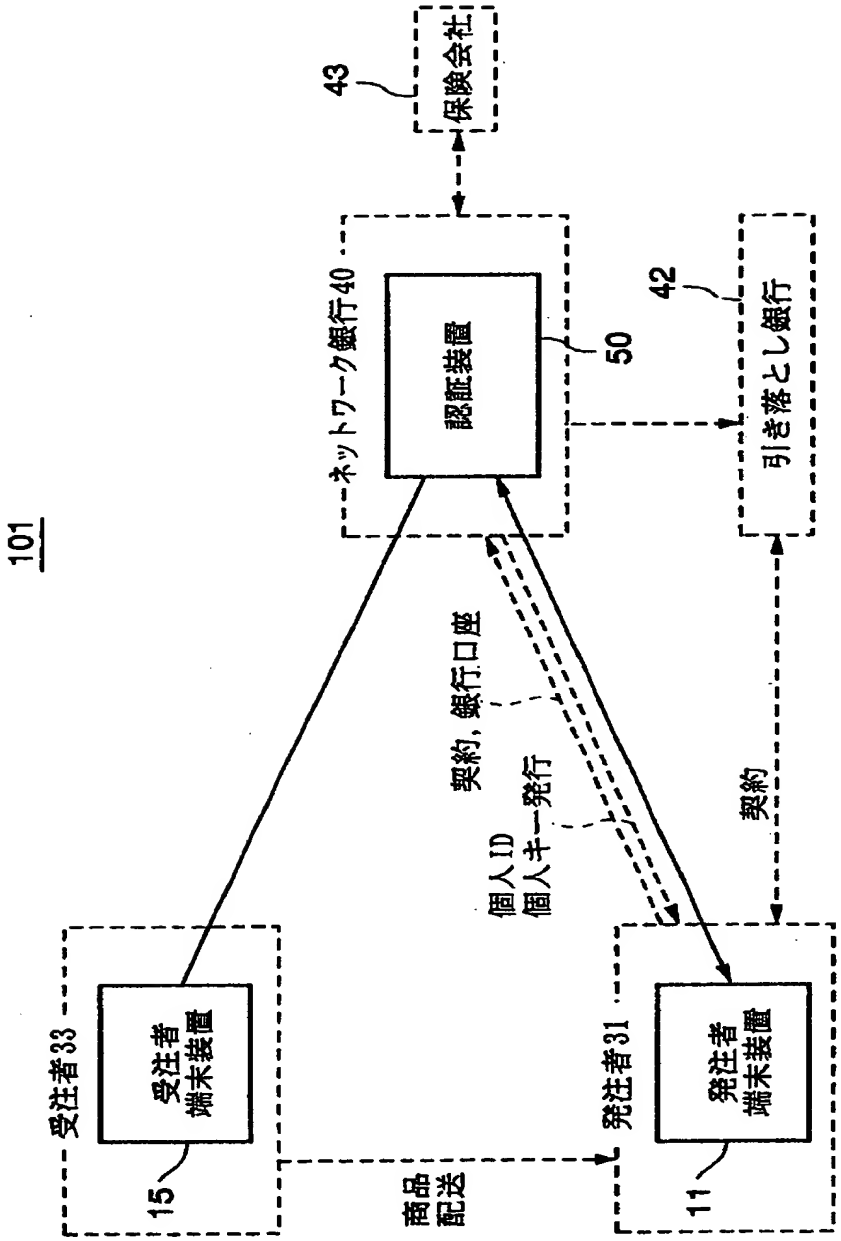
図５は、図１に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【符号の説明】

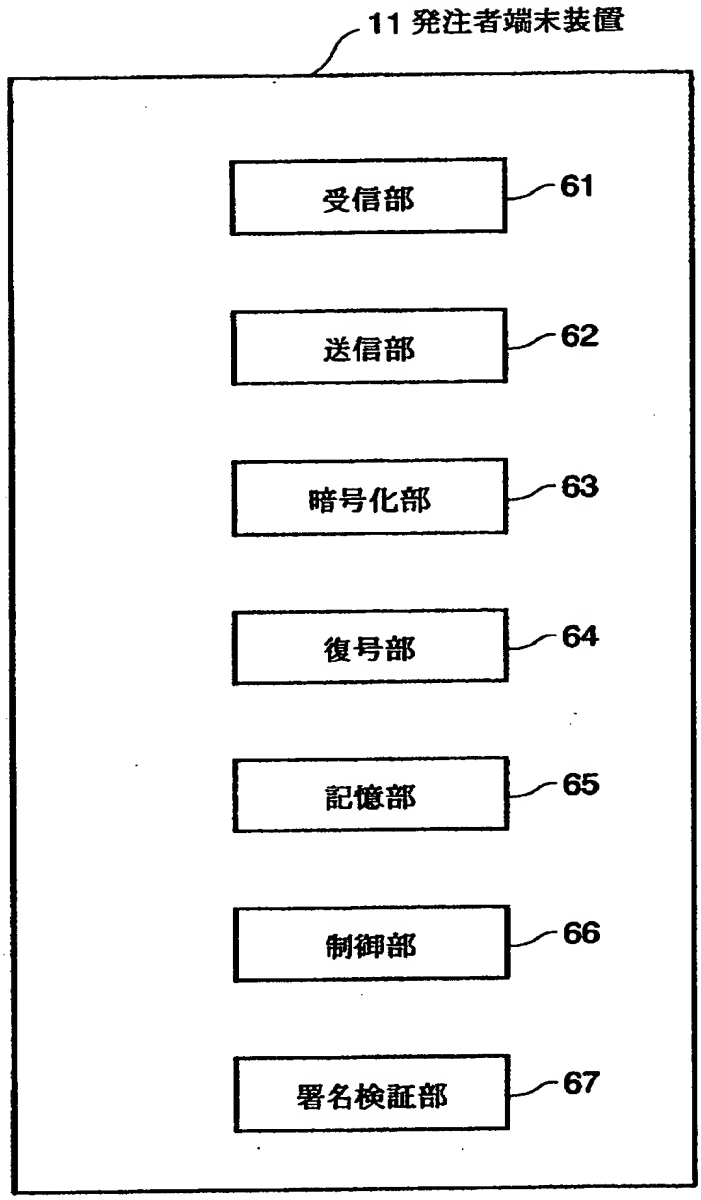
１…トランザクション認証システム、１１…発注者端末装置、１５…受注者端末装置、３１…発注者、３３…受注者、４０…ネットワーク銀行、５０…認証装置、６１，７１，８１…受信部、６２，７２，８２…送信部、６３，７３，８３…暗号化部、６４，７４，８４…復号部、６５，７５，８５…記憶部、６６，７６，８６…制御部、６７，７７…署名検証部、，８７…署名作成部、８８…課金処理部、ａ１…発注情報、ｋ１…発注者３１の個人キー情報ｋ１、ＩＤ１…発注者３１の個人ＩＤ情報、ID_M…装置ＩＤ情報、Ａｕ１，Ａｕ２…認証装置の署名情報、Ｚ…受注者の個人キー情報、Ｉｎｆ１…認証要求、Ｉｎｆ４…認証応答

【書類名】　図面

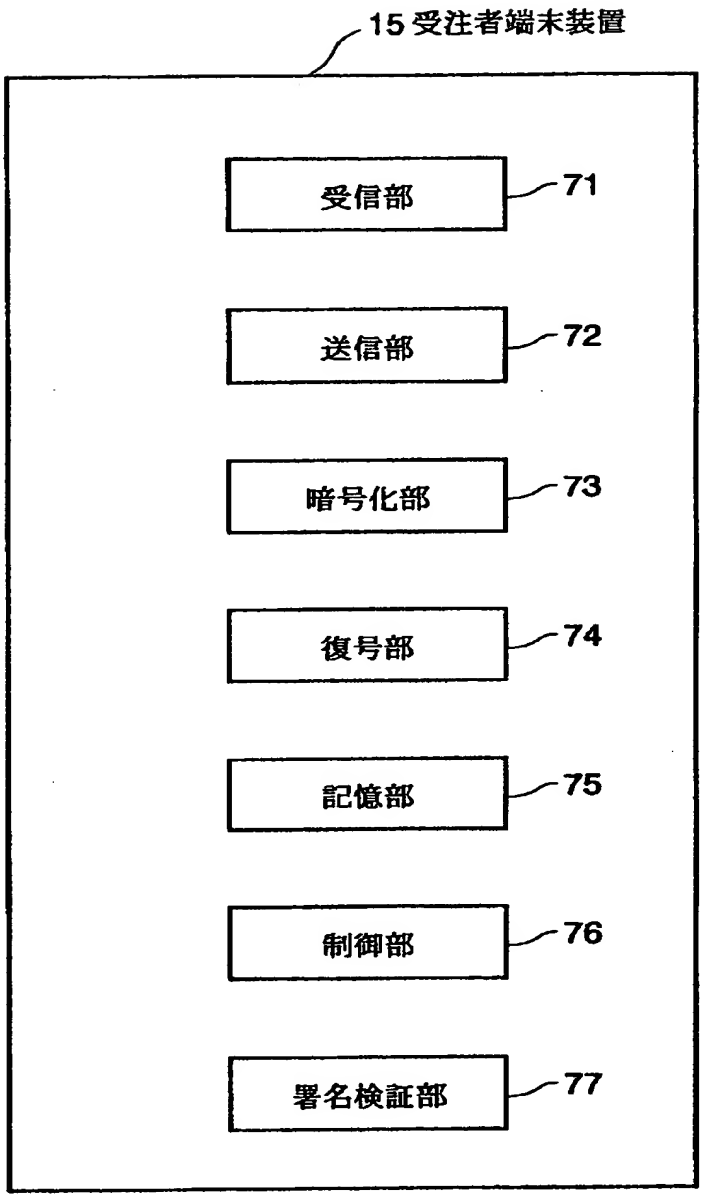
【図１】


101
43
保険会社
ネットワーク銀行40
認証装置
50
42
引き落とし銀行
契約，銀行口座
個人ID
個人キー発行
契約
受注者33
受注者
端末装置
15
商品
配送
発注者31
発注者
端末装置
11

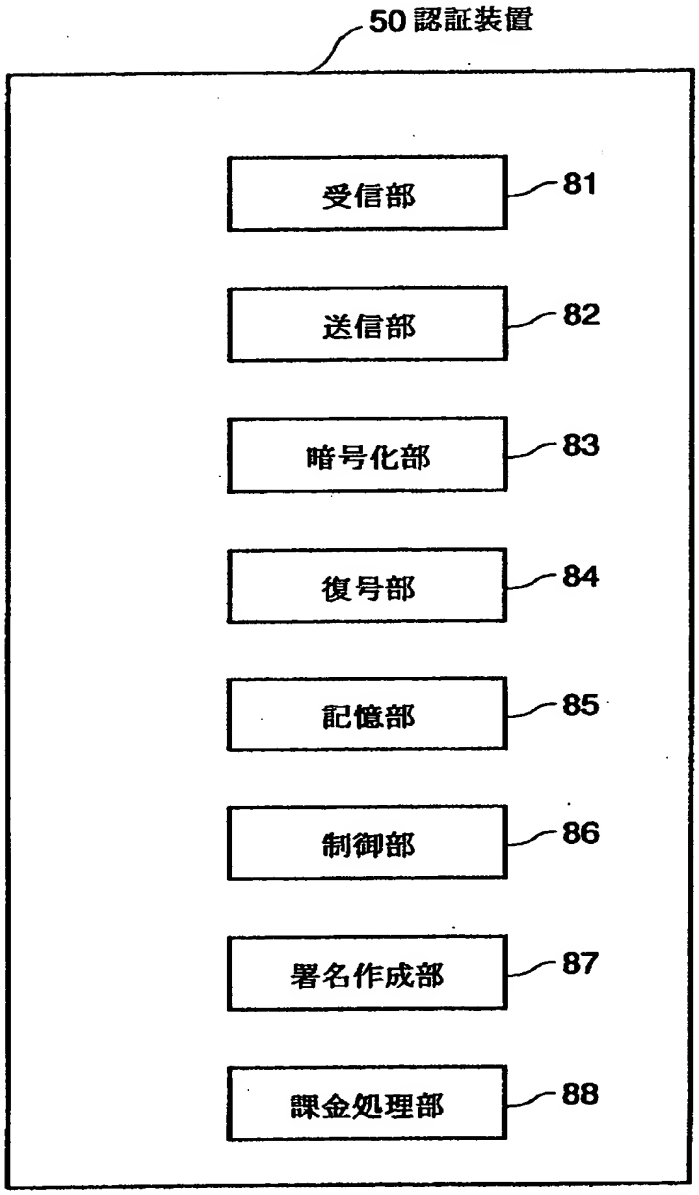
【図２】



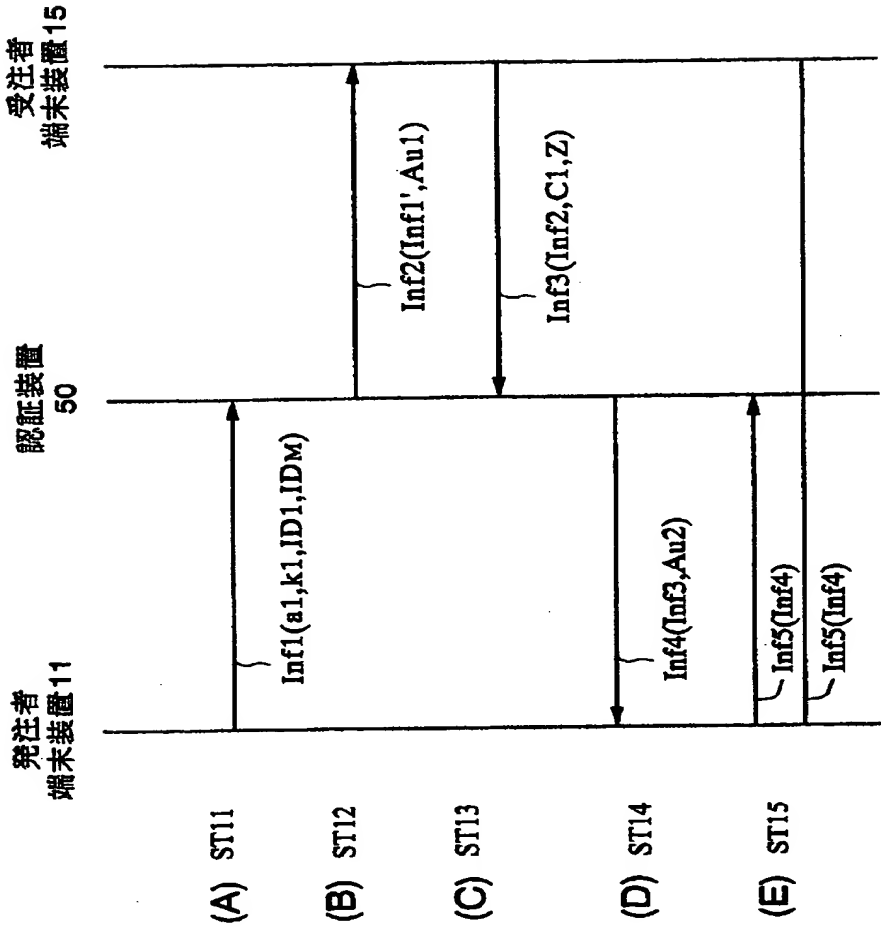
【図３】



【図４】


50 認証装置
受信部
81
送信部
82
暗号化部
83
復号部
84
記憶部
85
制御部
86
署名作成部
87
課金処理部
88

【図５】


受注者
端末装置15
認証装置
50
発注者
端末装置11
Inf1(a1,k1,ID1,IDM)
Inf2(Inf1',Au1)
Inf3(Inf2,C1,Z)
Inf4(Inf3,Au2)
Inf5(Inf4)
Inf5(Inf4)
(A) ST11
(B) ST12
(C) ST13
(D) ST14
(E) ST15

【書類名】　　要約書

【要約】

【課題】　不正に取得した他人の個人ＩＤ情報に基づいて不正な認証手続が行われることを回避する認証装置を提供する。

【解決手段】　認証装置５０は、発注者端末装置１１からの認証要求によって、発注者端末装置１１を特定する装置ＩＤ情報$ＩＤ_{M}$と、発注者３１を特定する個人ＩＤ情報等とを受信し、受注者端末装置１５との間の通信を行った後に、認証要求に含まれた装置ＩＤ情報$ＩＤ_{M}$を含む認証応答を発注者端末装置１１に送信する。発注者端末装置１１では、当該認証応答に含まれた装置ＩＤ情報$ＩＤ_{M}$が自らの装置ＩＤ情報$ＩＤ_{M}$と一致するかを確認する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
　［変更理由］　新規登録
　　住　所　　東京都品川区北品川６丁目７番３５号
　　氏　名　　ソニー株式会社